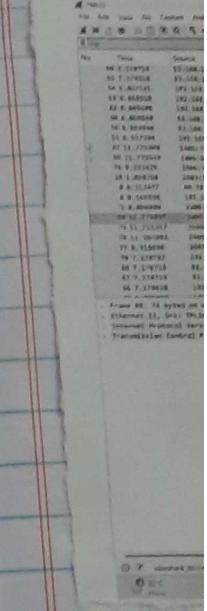
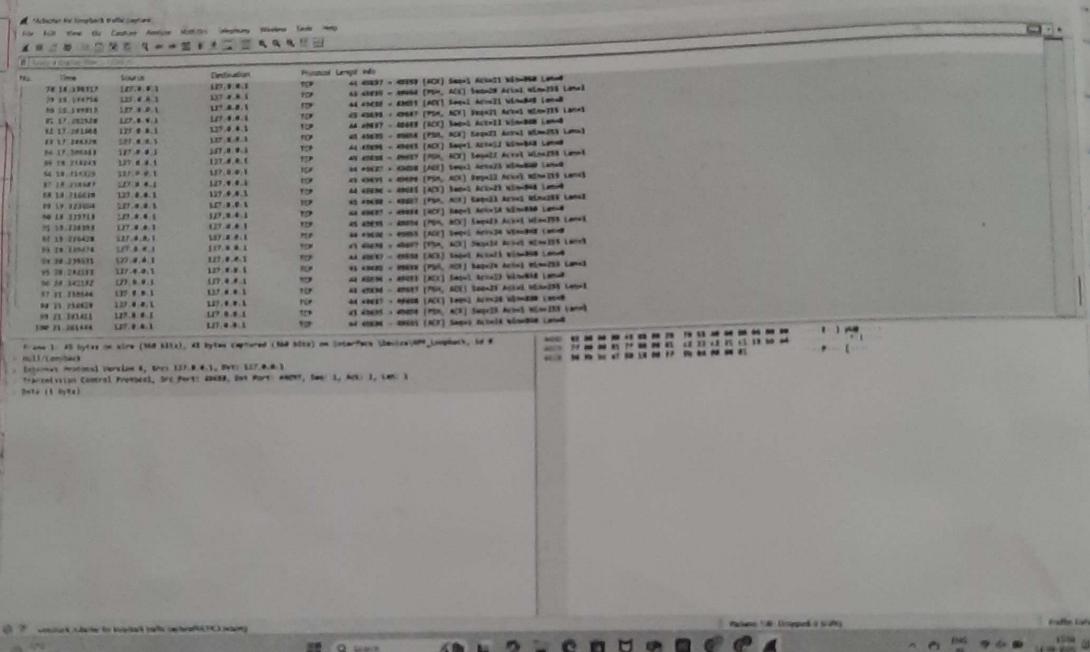


Ex 4: Experiments on Packet Capture tool: Wireshark

Aim: To understand the features of wireshark as a packet capture tool and understand encapsulation of information.



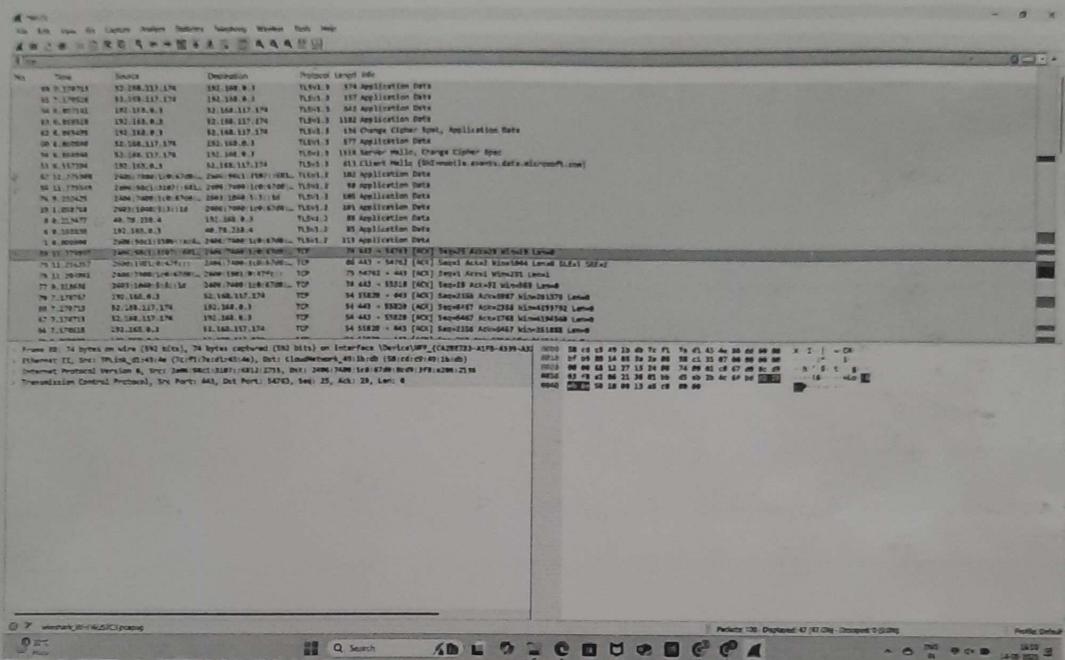
1. Create a filter to display only TCP/UDP packets, inspect the packets and provide the flow graph.

2. Create packet process

Procedure:

- Select Local Area Connection in wireshark.
- Go the capture → option
- Select stop capture automatically after 100 packets

- Then click Start capture
- Search TCP packets in search bar
- To see flow graph click statistics → Flow graph
- To see flow G
- Save the packets



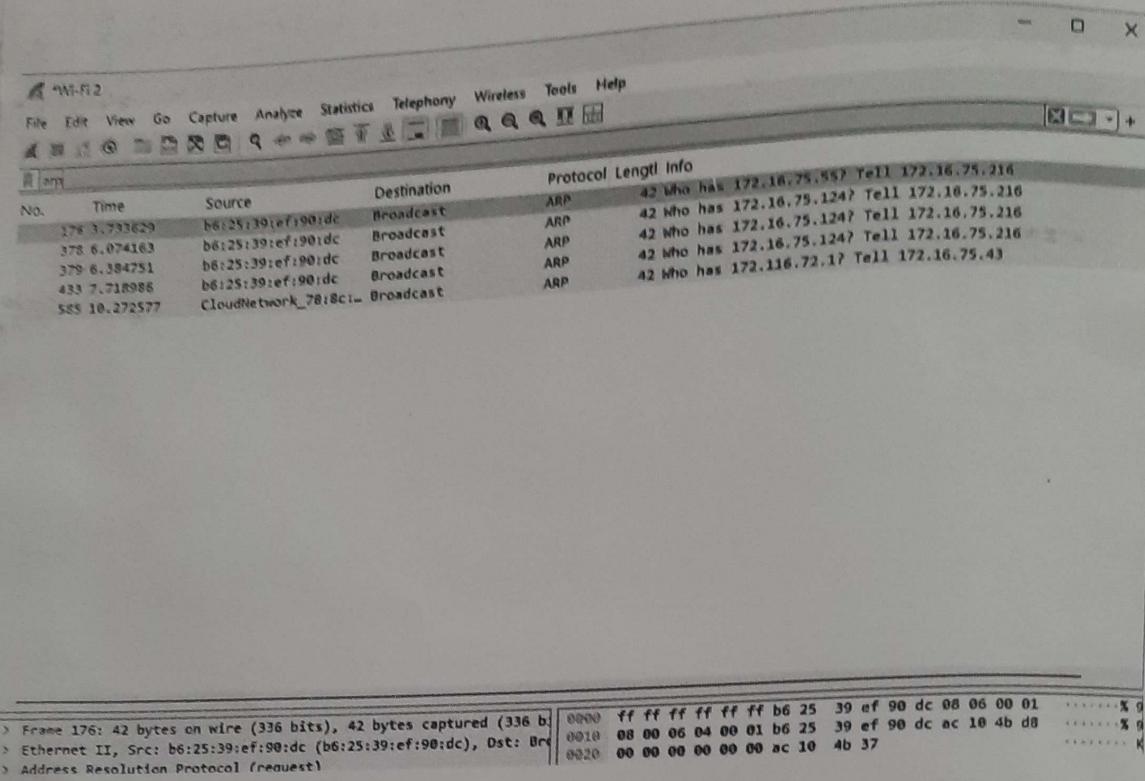
26

2. Create a filter to display only ARP packets and inspect the packets

Procedure

- Go to capture → option
- select stop capture automatically after 100 packets
- Then click start capture
- Search ARP packets in search bar

→ Save the packet.



3. Create a filter to display only DNS packets and provide the flow graph procedure.

→ Go to capture → Option

→ Select stop capture automatically after 100 packets.

! → Then click start capture

→ Search DNS packets in search bar

→ To see flow graph click statistics → Flow graph.

→ Save the packet.

No.	Time	Source	Destination	Protocol	Length	Info
2015	51.767745	172.16.75.98	172.16.72.1	DNS	78	Standard query 0x0022 A g.live.com
2016	52.854097	172.16.72.1	172.16.75.98	DNS	140	Standard query response 0x0022 A g.live.com DNSR 0x0001
2018	52.383106	172.16.75.98	172.16.72.1	DNS	76	Standard query 0x003f A mailclient.office.com
2019	52.383493	172.16.72.1	172.16.75.98	DNS	103	Standard query response 0x003f A mailclient.office.com DNSR 0x0001
3038	52.851922	172.16.75.98	172.16.72.1	DNS	74	Standard query 0x0045 A ecz.office.com
3039	52.866648	172.16.72.1	172.16.75.98	DNS	253	Standard query response 0x0045 A ecz.office.com DNSR 0x0001
3645	63.738285	172.16.75.98	172.16.72.1	DNS	92	Standard query 0x0f32 A Watson.events.data.microsoft.com
3646	63.868674	172.16.72.1	172.16.75.98	DNS	214	Standard query response 0x0f32 A Watson.events.data.microsoft.com DNSR 0x0001
4012	68.977429	172.16.75.98	8.8.8.8	DNS	78	Standard query 0x04ff A dns.google
4023	68.977725	172.16.75.98	8.8.8.8	DNS	78	Standard query 0x0751 HTTPS dns.google
4014	69.102892	8.8.8.8	172.16.75.98	DNS	146	Standard query response 0x0751 HTTPS dns.google SDA ncl_1
4015	69.102892	8.8.8.8	172.16.75.98	DNS	142	Standard query response 0x04ff A dns.google A 8.8.8.8 A 8

4. Create a filter to display only HTTP packets and inspect the packets

procedure:

- Select Local Area Connection in Network
- Go to capture → Options
- Select Stop capture automatically after 100 packets
- ~~Search - HTTP packets in Search bar~~
- Save the packets

No.	Time	Source	Destination	Protocol	Length	Info
2745	51.789745	172.16.75.98	172.16.72.1	DNS	79	Standard query 0x8d12 A g.live.com
2060	51.854697	172.16.72.1	172.16.75.98	DNS	148	Standard query response 0x8d12 A g.live.com CHNAME g.msn.c...
2806	52.063106	172.16.75.98	172.16.72.1	DNS	76	Standard query 0x533f A oneclient.sfx.ms
2817	52.389493	172.16.72.1	172.16.75.98	DNS	183	Standard query response 0x533f A oneclient.sfx.ms CHNAME o...
3038	52.851922	172.16.75.98	172.16.72.1	DNS	74	Standard query 0x6845 A ecs.office.com
3039	52.856648	172.16.72.1	172.16.75.98	DNS	155	Standard query response 0x6845 A ecs.office.com CHNAME ecs...
3645	63.778285	172.16.75.98	172.16.72.1	DNS	92	Standard query 0xf152 A watson.events.data.microsoft.com
3646	63.868674	172.16.72.1	172.16.75.98	DNS	214	Standard query response 0xf152 A watson.events.data.microsoft...
4012	69.977429	172.16.75.98	8.8.8.8	DNS	78	Standard query 0xc40f A dns.google
4013	69.977735	172.16.75.98	8.8.8.8	DNS	146	Standard query response 0x1751 HTTPS dns.google
4024	69.182852	8.8.8.8	172.16.75.98	DNS	102	Standard query response 0xc40f A dns.google A 8.8.8.8 A 8...
4035	69.382892	8.8.8.8	172.16.75.98	DNS		

5) Create a filter to display only IP/ICMP P packets and inspect the packets.

Procedure:

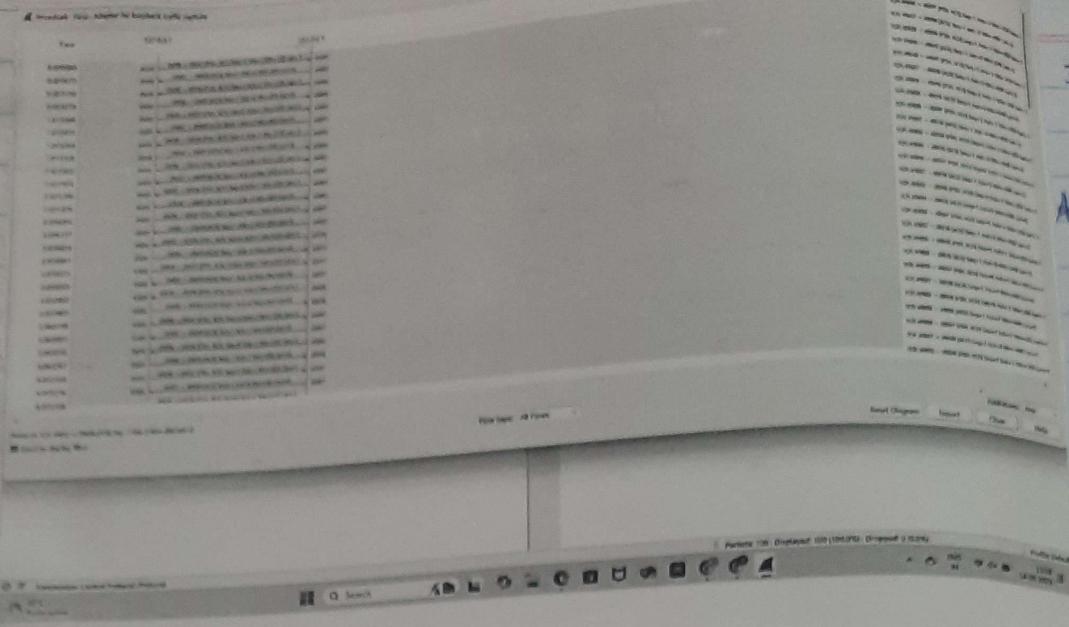
- Select local Area Connection in Wireshark
- Go to capture → Option
- Select stop capture automatically after 100 packets.
- then click Start capture
- Search ICMP P/IP packets in search bar.
- Save the packets

6) Create a filter to display only DHCP
packets and inspect the packets

Procedure

- ~~capture~~

 - Select Local Area Connection in Wireshark
 - Go to capture → Options
 - Select Stop capture automatically after 100 packets
 - Then click start capture
 - Search DHCP packets in search bar
 - Save the packets.



3) Which layer is involved by DNS
Ans: DNS layer

4) What is the protocol used?
Ans: http

Ans: http

5) What is promiscuous mode?

Ans: A network interface mode where a device captures all network traffic it sees, not just packets addressed to it.

1.) what is promiscuous mode?

Ans: A network interface mode where a device captures all network traffic it sees, not just packets addressed to it.

2) Does ARP packets have transport layer header? Explain

Ans: ARP packets do not have a transport layer header. They operate at the link layer (Layer 2) and are used to map IP address to MAC address without involving transport layer protocols like TCP or UDP.

3) Which transport layer protocol is used by DNS?

Ans: DNS primarily uses UDP for queries and responses, but can use TCP for larger responses or zone transfers.

4) What is the port number used by http protocol?

Ans: http uses port 80

5) What is broadcast IP address?

Ans: A broadcast IP address is used to send data to all devices in a network, typically that the last address in a subnet (e.g.; 192.168.1.255 for 192.168.1.0/24) network.

Result:

This experiment is performed in Wireshark, is impl